FEE TRANSMITTAL for FY 2005

Patent fees are subject to annual revision.

☐ Applicant claims small entity status. See 37 CFR 1.27.

TOTAL AMOUNT OF PAYMENT	($)	500.00

Complete if Known	
Application Number	10/025,088
Filing Date	December 18, 2001
First Named Inventor	Roy Want
Examiner Name	Smith, Sheila B.
Art Unit	2617
Attorney Docket No.	42390P12019

METHOD OF PAYMENT *(check all that apply)*

☒ Check ☐ Credit card ☐ Money Order ☐ None ☐ Other (please identify): _____

☒ Deposit Account Deposit Account Number: 02-2666 Deposit Account Name: Blakely, Sokoloff, Taylor & Zafman LLP

For the above-identified deposit account, the Director is hereby authorized to: (check all that apply)

☐ Charge fee(s) indicated below
☒ Charge any additional fee(s) or underpayment of fee(s) under 37 CFR §§ 1.16, 1.17, 1.18 and 1.20.
☐ Charge fee(s) indicated below, except for the filing fee
☒ Credit any overpayments

FEE CALCULATION

Large Entity Fee Code	Large Entity Fee ($)	Small Entity Fee Code	Small Entity Fee ($)	Fee Description	Fee Paid
1051	130	2051	65	Surcharge - late filing fee or oath	
1052	50	2052	25	Surcharge - late provisional filing fee or cover sheet.	
2053	130	2053	130	Non-English specification	
1251	120	2251	60	Extension for reply within first month	
1252	450	2252	225	Extension for reply within second month	
1253	1,020	2253	510	Extension for reply within third month	
1254	1,590	2254	795	Extension for reply within fourth month	
1255	2,160	2255	1,080	Extension for reply within fifth month	
1401	500	2401	250	Notice of Appeal	
1402	500	2402	250	Filing a brief in support of an appeal	500.00
1403		2403		Request for oral hearing	
1451		2451		Petition to institute a public use proceeding	
1460		2460		Petitions to the Commissioner	
1807	50	1807	50	Processing fee under 37 CFR 1.17(q)	
1806	180	1806	180	Submission of Information Disclosure Stmt	
1809	790	1809	395	Filing a submission after final rejection (37 CFR § 1.129(a))	
1810	790	2810	395	For each additional invention to be examined (37 CFR § 1.129(b))	
				Other fee (specify) _____	
				SUBTOTAL (2)	($) 500.00

SUBMITTED BY Complete (if applicable)

Name (Print/Type)	Mark L. Watson	Registration No. (Attorney/Agent)	46,322	Telephone	(303) 740-1980
Signature				Date	08/21/06

Based on PTO/SB/17 (12-04) as modified by Blakely, Sokoloff, Taylor & Zafman (wlr) 12/15/2004.
SEND TO: Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

AF/2617/ZFW

Patent

IN THE UNITED STATES PATENT AND TRADEMARK OFFICE
BEFORE THE BOARD OF PATENT APPEALS AND INTERFERENCES

In re Application of:

Want) Examiner: Smith, Sheila B.

Application No.: 10/025,088) **Art Group: 2617**

Filed: December 18, 2001)

For: Method and Device for Communicating Data)

Mail Stop Appeal Brief – Patents
Commissioner for Patents
P.O. Box 1450
Alexandria, VA 22313-1450

APPEAL BRIEF
IN SUPPORT OF APPELLANT'S APPEAL
TO THE BOARD OF PATENT APPEALS AND INTERFERENCES

Sir:

Applicant (hereinafter "Appellant") hereby submits this Brief in support of its appeal from a final decision by the Examiner, mailed March 23, 2006, in the above-captioned case. Appellant respectfully requests consideration of this appeal by the Board of Patent Appeals and Interferences (hereinafter "Board") for allowance of the above-captioned patent application.

An oral hearing is not desired.

08/29/2006 CNGUYEN2 00000004 10025088
01 FC:1402 500.00 OP

TABLE OF CONTENTS

I. REAL PARTY IN INTEREST

The invention is assigned to Intel Corporation, 2200 Mission College Boulevard, Santa Clara, California 95052, USA.

II. RELATED APPEALS AND INTERFERENCES

To the best of Appellant's knowledge, there are no appeals or interferences related to the present appeal that will directly affect, be directly affected by, or have a bearing on the Board's decision.

III. STATUS OF THE CLAIMS

Claims 1, 3-15 and 17-42 are currently pending in the above-referenced application. No claims have been allowed. Claims 1, 3-15 and 17-42 are the subject of this appeal.

IV. STATUS OF AMENDMENTS

In response to a Final Office Action, mailed on March 23, 2006, rejecting claims 1, 3-15 and 17-42, Appellant filed a Response After Final under 37 C.F.R. §1.116 on April 18, 2006. Appellant filed a Notice of Appeal on June 23, 2006.

A copy of all claims on appeal is attached hereto as an Appendix of Claims.

V. SUMMARY OF THE INVENTION

According to one embodiment, a portable device is disclosed. The device includes a wireless communication module to communicate with each of a plurality of remote devices within a locality, a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner. Further, the device includes a controller connected to the wireless communication module and to the data storage module to establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area. See Figure 1 and Specification at page 1, line 1 – page 2, line 16.

According to another embodiment, a data communication system includes a plurality of remote devices, where each remote device including a wireless communication interface and at least one portable device. The portable device includes a wireless communication module to communicate within a locality with the wireless communication interface the remote devices a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner, The device also includes a controller connected to the wireless communication module and to the data storage module to establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area. See Figure 1 and Specification at page 1, line 1 – page 2, line 16.

In yet a further embodiment a method includes monitoring, by means of a portable device, wireless communications from a plurality of remote devices requesting communications with the portable device within a locality. The portable device includes a public storage area with which selected remote devices exchange data in a free manner and a private storage area with which selected remote devices exchange data in a restricted manner. The method also includes identifying access rights associated with the remote device; and establishing a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area. See Figures 3 and 4.

In still a further embodiment, a computer program product is disclosed including a medium readable by a computer, the medium carrying instructions which, when executed by the computer, cause the computer to monitor wireless communications within a locality from a plurality of remote devices requesting substantive communications with a portable device including the processor and a data storage module a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner, identify access rights associated with the remote device and establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area. See Figures 3 and 4.

VI. GROUNDS OF REJECTION TO BE REVIEWED ON APPEAL

Claims 1, 3-15 and 17-42 stand rejected under 35 U.S.C. §103(a) as being unpatentable over Tobin (U.S. Pub. No. 2002/0077992) (hereinafter "*Tobin*") in view of Keenan (U.S. Patent No. 6,788,934) (hereinafter "*Keenan*").

VII. ARGUMENTS

1. THE PENDING CLAIMS WERE IMPROPERLY REJECTED UNDER 35 U.S.C. § 103(a) BECAUSE THE COMBINATION OF *TOBIN* AND *KEENAN* DO NOT DISCLOSE OR SUGGEST EACH AND EVERY FEATURE OF THE PENDING CLAIMS

Appellant respectfully submits that the combination of *Tobin* and *Keenan* fails to disclose or suggest the claimed invention for the reasons set forth below. As the Honorable Board is well aware, in order to establish a *prima facie* case of obviousness:

First, there must be some suggestion or motivation, either in the references themselves or in the knowledge generally available to one of ordinary skill in the art, to modify the reference or to combine reference teachings. Second, there must be a reasonable expectation of success. Finally, *the prior art reference (or references when combined) must teach or suggest all the claim limitations*." (Emphasis added). *In re Vaech*, 947 F.2d 488, 20 USPQ2d 1438 (Fed. Cir. 1991). Manual of Patent Examining Procedure (MPEP), 8th Edition, Revision 2, May 2004, §2143.

(A) Claims 1, 3-15 and 17-42 were improperly rejected because the combination of *Tobin* and *Keenan* does not disclose or suggest a controller to establish a wireless communication link between a wireless communication module and a first remote device based upon access rights associated with the first remote device to a public storage area and a private storage area

Claims 1, 3-15 and 17-42 are not obvious in view of *Tobin* and *Keenan* under 35 U.S.C. § 103(a). For example, Appellant's claim 1 recites:

> A portable device, which includes:
> a wireless communication module to communicate with each of a plurality of remote devices within a locality;
> a data storage module having a public storage area with which selected remote devices exchange data in a

free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and

a controller connected to the wireless communication module and to the data storage module, to establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

Appellant's claim 15 recites:

A data communication system, which includes:

a plurality of remote devices, each remote device including a wireless communication interface; and

at least one portable device, which includes:

a wireless communication module to communicate within a locality with the wireless communication interface the remote devices;

a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and

a controller connected to the wireless communication module and to the data storage module, to establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

Appellant's claim 21 recites:

A method which includes:

monitoring, by means of a portable device, wireless communications from a plurality of remote devices requesting communications with the portable device within a locality, the portable device including a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;

identifying access rights associated with the remote device; and

establishing a wireless communication link between

the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

Appellant's claim 32 recites:

> A computer program product including a medium readable by a computer, the medium carrying instructions which, when executed by the computer, cause the computer to:
>
> monitor wireless communications within a locality from a plurality of remote devices requesting substantive communications with a portable device including the processor and a data storage module a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;
>
> identify access rights associated with the remote device; and
>
> establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

Tobin discloses an electronic system that includes a user transaction device that provides a device identifier when coupled to a transaction terminal. The transaction terminal is configured to indicate that a transaction is to be performed when coupled to the user transaction device. The electronic system also includes a transaction privacy clearinghouse (TPCH), coupled selectively to the user transaction device when a transaction is to be performed. The TPCH is coupled to receive the device identifier and accessible data. Additionally, the accessible data is to be stored in a public storage area of a memory storage device that can be communicatively coupled to the user transaction device. The TPCH authorizes a transaction based upon the device identifier and the accessible data that includes account information of a user that is authorized to use the

user transaction device. Moreover, a transaction is authorized without providing the identity of the user to the transaction terminal. The memory storage device also includes a private storage area for storage of confidential data such that the private storage area is to be encrypted with a key that is to be stored in the user transaction device. See *Tobin* at paragraph [0007].

Keenan discloses a system for centrally and remotely testing switches of cellular and conventional telecommunications network wherein a controller located at a remote location provides instructions to Remote Call Processor (RCP) to thereby prompt the RCPs to establish a communication link from the RCP through a switch to a destination device whereby audio from said destination device is communicated, by way of the switch and the RCP, to the controller in order to verify that the switch properly routed and billed of the call. The destination device may be a service provided by such network or it may be another RCP. See *Keenan* at Abstract.

Appellant submits that any combination of *Tobin* and *Keenan* fails to disclose or suggest a controller to establish a wireless communication link between a wireless communication module and a first remote device based upon access rights associated with the first remote device to a public storage area and a private storage area. In fact, the Examiner admits that *Tobin* does not disclose a wireless communication link between a wireless device and a first remote device. See the Final Office Action at page 3, lines 1-2. Instead, the Examiner asserts that *Keenan* discloses a controller to establish a wireless communication link between a wireless communication module and a first remote device. Id. at lines 3-6.

As discussed above, *Keenan* discloses a controller located at a remote location that provides instructions to a RCP to prompt the RCPs to establish a communication link through a switch to a destination device. However, there is no disclosure that the controller in Keenan establishes the communication link based upon access rights associated with the first remote device to a public storage area and a private storage area. Since neither reference discloses or suggests establishing a wireless communication link between a wireless communication module and a first remote device based upon access rights associated with the first remote device to a public storage area and a private storage area, any combination of *Tobin* and *Keenan* would also not disclose or suggest such a feature.

Further, Appellant submits that there is no motivation provided in any of the references themselves to combine *Tobin* and *Keenan*. Particularly, it would be impermissible hindsight based on Appellant's own disclosure to incorporate the personal transaction device in *Tobin* into the *Keenan* test system for remotely testing switches within a telecommunications network. As a result, the combining of *Tobin* and *Keenan* is not a proper combination under §103.

Consequently, the Examiner has not established a prima facie case of obviousness, and the Examiner's rejection of claims 1, 15, 21 and 32 under 35 U.S.C. §103(a) as being obvious over the combination of *Tobin* and *Keenan*.

Claims 3-14 depend from claim 1, claims 17-20 depend from claim 15, claims 22-31 depend from claim 21 and claims 33-42 depend from claim 32. Given that dependent claims necessarily include the limitations of the claims from which they depend,

Appellant submits that the invention as claimed in claims 3-14, 17-20, 22-31 and 33-42 are similarly patentable over the combination of *Tobin* and *Keenan*.

For the forgoing reasons, Appellant submits that the Examiner has failed to search and find a printed publication or patent that discloses the claimed invention as set forth in MPEP § 706.02(a).

Thus, the Examiner erred in rejecting claims 1-24 under 35 U.S.C. § 103(a).

VIII. CONCLUSION

Appellant respectfully submits that all the appealed claims in this application are patentable and request that the Board of Patent Appeals and Interferences overrule the Examiner and direct allowance of the rejected claims.

This brief is submitted, along with a check for $500.00 to cover the appeal fee for one other than a small entity as specified in 37 C.F.R. § 1.17(c). Please charge any shortages and credit any overpayment to out Deposit Account No. 02-2666.

Respectfully submitted,

BLAKELY, SOKOLOFF, TAYLOR & ZAFMAN

Date: August 21, 2006

Mark L. Watson
Attorney for Appellant
Reg. No. 46,322

12400 Wilshire Boulevard
Seventh Floor
Los Angeles, CA 90025-1030
(303) 740-1980

FIRST CLASS CERTIFICATE OF MAILING

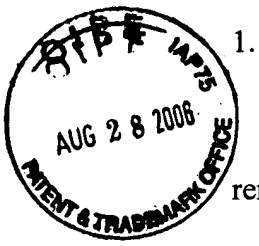
I hereby certify that I am causing the above-referenced correspondence to be deposited with the United States Postal Service as first class mail with sufficient postage on the date indicated below and that this paper or fee has been addressed to the Commissioner for Patents, P.O. Box 1450, Alexandria, VA 22313-1450

Date of Deposit: August 21, 2006.

Name of Person Mailing Correspondence: Leah Schwenke

Leah Schwenke — 8/21/06

Signature — Date



IX. APPENDIX OF CLAIMS (37 C.F.R. § 1.192(c)(9))

1. A portable device, which includes:

a wireless communication module to communicate with each of a plurality of remote devices within a locality;

a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and

a controller connected to the wireless communication module and to the data storage module, to establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

2. (Canceled)

3. A portable device as claimed in Claim 1, in which the controller filters requests from each of the remote devices to exchange data and to reject and accept the requests in response to the nature of services offered by the remote device.

4. A portable device as claimed in Claim 1, in which the controller defines access rights to the first and second storage areas and, dependent upon the access rights, allows the remote device to store and retrieve data from at least one of the first and second storage areas.

5. A portable device as claimed in Claim 1, in which a digital certificate of authenticity is requested from the remote device prior to communicating data between the remote device and the private storage area.

6. A portable device as claimed in Claim 1, in which the controller restricts how often and the amount of data which is writable by the remote device into the public storage area.

7. A portable device as claimed in Claim 1, in which data stored in the public storage area is selectively cleared by the controller in an automated fashion.

8. A portable device as claimed in Claim 1, in which the portable device and the remote device communicate using secure sockets layer (SSL) protocols.

9. A portable device as claimed in Claim 1, which detects Universal Plug and Play (UPnP) broadcasts.

10. A portable device as claimed in Claim 1, in which the wireless communication module is a radio frequency (RF) transceiver which communicates using a standardized communication protocol.

11. A portable device as claimed in Claim 10, in which the standardized communication protocol is selected from the group including Bluetooth IEEE 802.15 technology, IEEE 802.11a technology, and IEEE 802.11b technology.

12. A portable device as claimed in Claim 1, in which the controller interfaces the portable device to a computer system to permit a user to access and store data in the data storage module.

13. A device as claimed in Claim 1, in which the remote device is defined by another portable device within the locality.

14. A device as claimed in Claim 1, which includes a rechargeable power supply for powering its various components.

15. A data communication system, which includes:

a plurality of remote devices, each remote device including a wireless communication interface; and

at least one portable device, which includes:

a wireless communication module to communicate within a locality with the wireless communication interface the remote devices;

a data storage module having a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner; and

a controller connected to the wireless communication module and to the data storage module, to establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

16. (Canceled)

17. A system as claimed in Claim 15, in which the controller filters requests from each of the remote devices to exchange data and to selectively reject and accept the requests in response to the nature of services offered by the remote device.

18. A system as claimed in Claim 15, in which the controller defines access rights to the first and second storage areas and, dependent upon the access rights, allows the remote device to store and retrieve data from at least one of the first and second storage areas.

19. A system as claimed in Claim 15, in which a digital certificate of authenticity is requested from the remote device prior to communicating data between the remote device and the private storage area.

20. A system as claimed in Claim 15, in which the controller restricts the amount of data which is writable by the remote device into the public storage area.

21. A method which includes:

monitoring, by means of a portable device, wireless communications from a plurality of remote devices requesting communications with the portable device within a locality, the portable device including a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;

identifying access rights associated with the remote device; and

establishing a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

22. A method as claimed in Claim 21, which includes exchanging data in a relatively free manner between the first storage area, which defines a public data storage area, and the remote device, and exchanging data in a relatively restricted manner between the second storage area, which defines a private data storage area, and the remote device.

23. A method as claimed in Claim 21, which includes:

filtering requests for substantive communications from each of the remote devices with the portable device ; and

selectively rejecting and accepting the requests in response to the nature of services offered by the remote device.

24. A method as claimed in Claim 22, which includes defining access rights to the first and second storage areas and, dependent upon the access rights, allowing the remote device to store and retrieve data from at least one of the first and second storage areas.

25. A method as claimed in Claim 24, in which the access rights are dependent upon a classification of the remote device by the portable device.

26. A method as claimed in Claim 22, which includes requesting a digital certificate of authenticity from the remote device prior to communicating data between the remote device and the private storage area.

27. A method as claimed in Claim 22, which includes restricting the amount of data which is writable by the remote devices into the public storage area.

28. A method as claimed in Claim 22, which includes selectively clearing data in the public storage area.

29. A method as claimed in Claim 21, which includes communicating between the portable device and the remote device using secure sockets layer (SSL) protocols.

30. A method as claimed in Claim 21, which includes detecting universal plug and play (UPnP) broadcasts from each remote device.

31. A method as claimed in Claim 21, which includes communicating via a radio frequency (RF) transceiver using a standardized communication protocol.

32. A method as claimed in Claim 31, which includes communicating using technology selected from the group including Bluetooth 802.15 technology, IEEE 802.11a technology and IEEE 802.11b technology.

33. A computer program product including a medium readable by a computer, the medium carrying instructions which, when executed by the computer, cause the computer to:

monitor wireless communications within a locality from a plurality of remote devices requesting substantive communications with a portable device including the processor and a data storage module a public storage area with which selected remote devices exchange data in a free manner, and a private storage area with which selected remote devices exchange data in a restricted manner;

identify access rights associated with the remote device; and

establish a wireless communication link between the wireless communication module and a first remote device based upon access rights associated with the first remote device to the public storage area and the private storage area.

34. A computer program product as claimed in Claim 33, in which data is exchanged in a relatively free manner between the first storage area, which defines a public data storage area, and the remote device, and data is exchanged in a relatively restricted manner between the second storage area, which defines a private data storage area, and the remote device.

35. A computer product as claimed in Claim 33, in which requests for substantive communications from each of the remote devices with the portable device are filtered, the requests being selectively rejected and accepted in response to the nature of services offered by the remote device.

36. A computer program product as claimed in Claim 33, which includes defining access rights to the first and second storage areas and, dependent upon the access rights, allowing the remote device to store and retrieve data from at least one of the first and second storage areas.

37. A computer program product as claimed in Claim 36, in which the access rights are dependent upon the classification of the remote device by the portable device.

38. A computer program product as claimed in Claim 34, which includes requesting a digital certificate of authenticity from the remote device prior to communicating data between the remote device and the private storage area.

39. A computer program product as claimed in Claim 34, which includes restricting how often and the amount of data which is writable by the remote devices into the public storage area.

40. A computer program product as claimed in Claim 34, which includes selectively clearing data in the public area.

41. A computer program product as claimed in Claim 33, which includes communicating between the portable device and the remote device using secure sockets layer (SSL) protocols.

42. A computer program product as claimed in Claim 33, which includes detecting universal plug and play (UPnP) broadcasts from each remote device.

X. EVIDENCE APPENDIX

None.

XI. RELATED PROCEEDINGS APPENDIX

None.